UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information associated with Apple ID Austin.brown.2323@icloud.com that is stored at premises controlled by Apple	))))	Case No. 21-MJ-452-KEW

APPLICATION FOR A SEARCH WARRANT

I, Amy Holt, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the **NORTHERN DISTRICT of CALIFORNIA**

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim P. 41(c) is *(check one or more)*:

X evidence of a crime;
X contraband, fruits of a crime, or other items illegally possessed;
❑ property designed for use, intended for use, or used in committing a crime;
❑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2243	Sexual abuse of a minor
18 U.S.C. § 2251	Attempted production of child pornography
18 U.S.C. § 2252A	Distribution and possession of child pornography
18 U.S.C. § 2422	Online enticement of a minor

The application is based on these facts: *see* attached Affidavit

X continued on the attached sheet
❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature
Amy Holt, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/10/2021

City and State: Muskogee, Oklahoma

Kimberly E. West
United States Magistrate Judge
Eastern District of Oklahoma

CJW:JEL

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH WARRANT

I, Amy Holt, the undersigned, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since August of 2020. I am currently assigned to the Oklahoma City Field Office, Muskogee Resident Agency, and work primarily Indian Country criminal investigations in the Eastern District of Oklahoma. As a Special Agent with the FBI, I am a law enforcement officer of the United States as defined by 18 U.S.C. § 2510(7), therefore, empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18 of the United States Code. Moreover, I am authorized to seek and execute federal arrest and search warrants for federal criminal offenses, including offenses related to the sexual abuse and exploitation of children.

2. As an FBI Agent, I have investigated Indian Country crimes to include a variety of violent crimes and child sexual assaults committed on the Muscogee (Creek) Nation Reservation, Cherokee Nation Reservation, and the Choctaw Nation Reservation. My investigative experience includes interviewing victims and witnesses, as well as conducting searches of physical locations, social media, and electronic devices pursuant to court order or consent. I have been trained in how to seek information using various court orders such as search warrants and orders pursuant 18 U.S.C. § 2703.

3. I make this affidavit in support of applications for search warrants for the following information that is controlled and maintained by Apple Inc. ("Apple"), which is headquartered at 1 Infinite Loop, Cupertino, CA 95014:

a. Information related to the account associated with Apple ID Austin.brown.2323@icloud.com ("**Target Account**"). This account is further described in the following paragraphs and in Attachment A. The information to be disclosed by Apple is described in Section I of Attachment B while the information to be seized by the government is described in Section II of Attachment B; and

4. The **Target Account** is believed to be associated with and/or utilized by **Austin Jae Brown** (**BROWN**), date of birth (DOB): XX/XX/1998.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2243 (sexual abuse of a minor), 18 U.S.C. § 2422 (online enticement of a minor), 18 U.S.C. §§ 2251 et seq. (attempted production, distribution, and possession of child pornography) have been committed by **BROWN**. There is also probable cause to search for information associated with the **Target Account** described in Attachment A for evidence of these crimes as further described in Attachment B.

6. The statements contained in this Affidavit are based in part on information provided by other agencies, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; independent investigation; and my experience, training, and background as a Special Agent with the FBI. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. In addition, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

PROBABLE CAUSE

7. On August 24, 2021, investigating agents at the FBI received an email from the Cherokee Nation Marshal Service stating that **BROWN**, confirmed Cherokee Nation citizen, had attempted to entice or persuade M.C. (DOB XX/XX/2006), confirmed Cherokee Nation citizen,

to perform oral sex via social media. Namely, **BROWN** had offered to meet with M.C. to "show her how to give head." M.C. told **BROWN** her age (14), and he portrayed himself as 16 years old. M.C. sent a photo of herself partially clothed on social media which **BROWN** threatened to send to M.C.'s coach to expose her.

8. Upon further investigation agents found numerous additional records, complaints and open investigations involving **BROWN** with similar allegations. The complaints alleged that **BROWN** would reach out to young women and girls on social media and ask them for pictures. If the females refused, **BROWN** would get angry. If they sent pictures, **BROWN** would threaten to share them if the girls did not meet with him in person. Review of the records and documents received revealed that **BROWN** used several different social media accounts. The records, complaints and open investigations originated from University of Arkansas Police Department, University of Central Arkansas Police Department, University of Oklahoma Police Department, Tuscaloosa Police Department, Canadian County Sheriff's Office, Choctaw Nation Lighthorse Police Department (CNLPD), Le Flore County Sheriff's Department and Stilwell Police Department.

9. In the reports received from Canadian County Sheriff's Office as well as the Tuscaloosa Police Department records, **BROWN**'s personal cell phone was associated with the email address Austin.brown.2323@icloud.com.

10. On September 29, 2021, investigators learned that CNLPD had opened an investigation on **BROWN** involving L.C. (DOB XX/XX/2007), confirmed Choctaw Nation citizen. CNLPD forensically interviewed L.C. who stated that she first talked to **BROWN** on or about December 29, 2020. L.C. lives in Talahina, OK, which is within the Choctaw Nation lands.

11. During the forensic interview L.C. stated that on or about the night of December 29, 2020, L.C. started talking with **BROWN** on social media and FaceTime. During the communications, **BROWN** told L.C. that he was 16. L.C. recalled telling him that she was 13. L.C. stated that she met up with **BROWN** and was with him from about 1:30 a.m. until approximately 6:00 a.m. While sitting in **BROWN's** car **BROWN** started kissing L.C. and placed her hand on his penis. L.C. said he told her to take her shirt off and indicated he wanted her to give him "head", so she did. After giving **BROWN** "head" L.C. was on his lap and felt his penis through his pants. L.C. stated that they then had intercourse. L.C. told **BROWN** to put a condom on but did not think that he did. L.C. recalled that she was laying in the back seat of his truck with **BROWN** on top while they had "intercourse".

12. L.C. went on to say that in January of 2021, **BROWN** came back multiple times, a couple of those times L.C. and **BROWN** had sex again. The last time L.C. had talked to **BROWN** was in the summer of 2021. **BROWN** contacted L.C. from different social media accounts to talk to her. **BROWN** sent L.C. nude photographs of himself and a video of a girl giving him "head" but L.C. did not ask for them and did not know who the girl was.

INFORMATION REGARDING APPLE AND iCLOUD[1]

13. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com;

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls;

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps;

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of

productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices;

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other;

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices;

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location;

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS;

15. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

16. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

17. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

18. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs"

for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

19. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

20. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS")

messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

21. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Additionally, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

22. In my training and experience, the types of information maintained by Apple may constitute evidence and instrumentalities of the crimes under investigation. Among other things, the requested information may assist in the identification of victims, other individuals engaged in sexual exploitation of minors and/or provide content relevant to the ongoing investigation of **BROWN**.

CONCLUSION

23. Based on the foregoing, I request that the Court issue the proposed search warrant.

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

by serving it on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Amy Holt, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me on December 10, 2021.

United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information related to the following Apple accounts, all of which is stored at premises controlled by Apple Inc. ("Apple" or "Provider"), headquartered at 1 Infinite Loop, Cupertino, CA 95014:

- Information related to the account associated with Apple ID Austin.brown.2323@icloud.com

This account will be referred to as the "Account" in Attachment B.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account(s) listed in Attachment A for the time period of December 1, 2020, until service of the Search Warrant:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and

accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.